Should you use a VPN on the Dark Web?

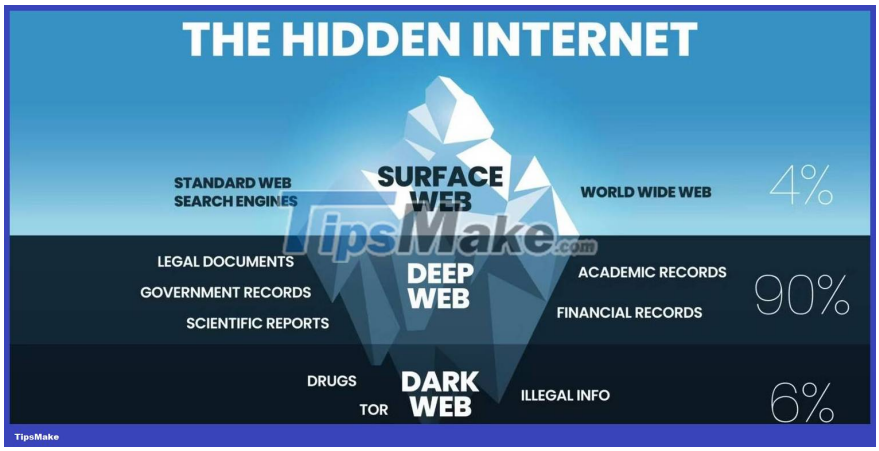
Are VPNs only useful for staying anonymous on regular websites and apps? If you're looking to dig deeper and access the dark web, is it worth using a VPN?

VPNs have become so popular over the past decade that even the most casual Internet users choose this security tool. But are VPNs only useful for staying anonymous on regular websites and apps? If you're looking to dig deeper and access the dark web, is it worth using a VPN?

How are the surface web, deep web and dark web different?

The Surface web is by far the most commonly used part of the World Wide Web. This includes all your usual sites, such as Facebook, HuffPost, Walmart, Netflix, and AliExpress. If you only use the Internet to talk to friends, buy goods and services, browse news, or stream content, chances are you've only ever used the surface web.

But the web is made up of many layers: Surface web, deep web and dark web. Some people even believe that deeper levels exist, such as the shadow web and Mariana's web.



What you may not know is that a shocking 90% of the web is made up of deep web content, including government records, scientific reports, financial records, and similar documents. An additional 6% were posted to the dark web, while only 4% comprised the surface web. Of course, these figures can change from year to year, but it's important to keep in mind that the surface web you're familiar with is only a small portion of the entire web.

Although the term "deep web" may sound a bit scary, much of this part of cyberspace is completely harmless. Much of this field consists of huge databases from all types of industries, such as those listed in the diagram

above. However, as is the case with the surface web, there are parts of the deep web that can pose a threat to you.

The next layer, the dark web, is a space filled with countless fears and rumors among the public. Many people consider this part of the web to be a completely illegal space, filled with bad content, drug and weapons markets, and stolen data.

In fact, the dark web contains these elements. Cybercriminals often visit the dark web to sell the data they have stolen, which could be passports, social security numbers, payment details or entire organizational databases. Paraphernalia can also be purchased on the dark web, such as class A drugs and illegal handguns. Some people turn to the dark web for its vast array of illegal content, such as banned movies, terrorist videos, and illegal pornography. Needless to say, the dark web encompasses a vast criminal underworld.

But beyond these shady aspects there is also harmless content. Many people use the dark web to conduct anonymous research, bypass national censorship, and access hard-to-find documents.

Regardless, there are still plenty of threats on the dark web that you don't want to encounter. So, should you use a VPN to avoid such risks?

Why should you use a VPN on the Dark Web?

The dark web is filled with dangerous and illegal websites. While this lower layer of the web can be used for harmless purposes, you should not ignore the range of dangers it can pose to anyone using it.

To access the dark web, you need to use Tor. This is a privacy-focused browser that can be used to surf the surface web, deep web, and dark web. Tor uses onion routing to keep users anonymous, but this is not the same as a VPN. Like a VPN, onion routing uses encryption and remote servers, but your data is sent to server locations you can't choose. However, onion routing encrypts your data 3 times, unlike most VPNs that only encrypt your data once.

Onion routing clearly focuses on keeping users anonymous. When accessing the dark web through Tor, you can benefit from the browser's enhanced privacy. However, privacy and security are not the same and this is an important factor to consider here.

Even if you are anonymous online, this does not make you 100% safe. Sure, your IP address and browsing activity may be hidden from other users and websites, but your device can still be infected with malware through dark web platforms. While many cybercriminals flock to the dark web as an illegal haven, others use it as a base to launch their attacks, especially because the agency Law enforcement cannot monitor the dark web as effectively as the surface web.

Additionally, using onion routing without a VPN will reveal your activity to your Internet service provider. Using Tor is not illegal, but if your ISP notices that you are using Tor regularly, they may consider your IP address suspicious. As a gateway to the dark web, Tor is known to be very popular among cybercriminals, so ISPs often keep an eye on users who frequently use this browser.

Furthermore, using Tor without a VPN enabled will expose your IP address to your browser's access node. In Tor's onion routing process, there are entry nodes, relay nodes, and exit nodes. Also known as the guard node, the entry node is the first port of call when you want to access a website.

Without using a VPN, you will access the entry node in raw form, meaning your IP address is viewable.

If you want to conduct research or access content anonymously, using Tor without a VPN can cause problems for you because you will be somewhat exposed through the entry node.

VPNs to avoid when using the Dark Web

If you want to use a VPN and the Tor browser (also known as Onion-over-VPN), there are many providers that will suit you, including ExpressVPN, SurfShark, ProtonVPN, and NordVPN.

However, there are many VPN services you should avoid when accessing the dark web. These include free and untested VPNs that can be considered dangerous.

First, free VPNs often have unimpressive features. Without large budgets from user fees, most free VPN providers cannot offer the best features, such as kill switches, top-level and double encryption, or additional perks. Additional features include ad blocking and malware scanning. If you're using the dark web, you want to make sure you're using a super secure VPN that can actually keep you safe. A paid, reputable VPN is the best choice.

You may also want to stay away from VPNs that haven't been independently tested. VPN providers may claim to have the best encryption, strict no-logs policy, and other great features, but only independent testing (i.e. testing by an unbiased third party) Only you can determine whether this is actually true or not. Some VPNs keep logs of user activity and IP addresses, which isn't ideal when you're using the dark web - especially if you want to be completely anonymous while doing so.

If you plan to visit riskier sites on the dark web, you'll want a VPN that's definitely safe.